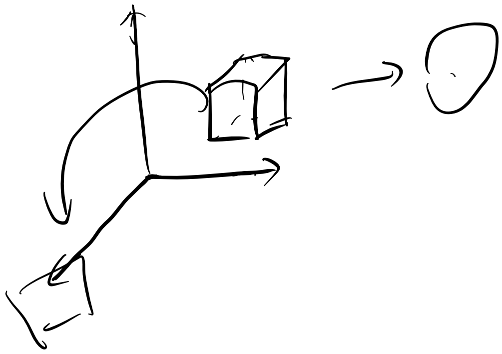


§1. Basic

Def 1.1. A group is a set G and a mapping from the Cartesian product $G \times G$ into G, which we will denote by juxtaposition:

$$G \times G \to G \ : (g_1, g_2) \mapsto g_1 g_2$$ multiplication law

with the following properties,

(1) Associativity: $g_1(g_2 g_3) = (g_1 g_2) g_3$. (结合律).

(2) Identity: $\exists e \in G$, s.t. $ea = ae = a$, $\forall a \in G$.

(3) Inverse: $\forall g \in G$, $\exists g^{-1} \in G$, s.t. $gg^{-1} = g^{-1}g = e$.

Exam 1.1. • $(\mathbb{R}, +)$

$\forall x_1, x_2, x_3 \in \mathbb{R}$, $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$. (1) ✓.

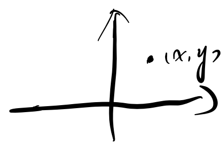
For $0 \in \mathbb{R}$, $\forall x \in \mathbb{R}$, $0 + x = x + 0 = x$. (2) ✓

$\forall x \in \mathbb{R}$, $\exists (-x) \in \mathbb{R}$, s.t. $x + (-x) = (-x) + x = 0$. (3) ✓

- Cartesian product: U, V

$$U \times V := \{ (u,v) : u \in U,\ v \in V \}.$$

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$$



$$U \times V \times W = \{ (u,v,w) : u \in U,\ v \in V,\ w \in W \}.$$

- $g_1 g_2 \neq g_2 g_1$ (general).

- $g_1 g_2 = g_1 \circ g_2 = g_1 \cdot g_2 = g_1 + g_2$

- The identity e is unique.

∴ If $e_1, e_2 \in G$ are identity of G, then

$$e_1 \overset{e_2 \text{ identity}}{=} e_1 e_2 \underset{e_1 \text{ identity}}{=} e_2$$

∵ If $e_1 \neq e_2 \in G$ ... $\Rightarrow$ $e_1 = e_2$ proof by contradiction

- $\forall g \in G$, g^{-1} unique.

If $h_1, h_2 \in G$ are the inverse of g.

$$g h_1 = h_1 g = e, \quad g h_2 = h_2 g = e.$$

$$h_1 = h_1 e = h_1 g h_2 = e h_2 = h_2.$$

- $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$

It suffices to show

$$(g_2^{-1}g_1^{-1})(g_1g_2) = (g_1g_2)(g_2^{-1}g_1^{-1}) = e.$$

$$\parallel$$

$$g_2^{-1}(g_1^{-1}g_1)g_2 = g_2^{-1}g_2 = e.$$

- $(g^{-1})^{-1} = g$

$$g^{-1}\cdot g = e.$$

Exam 1.1. $(\mathbb{Z}, +)$, $e = 0$

2 inverse -2.

? $(\mathbb{Z}, \cdot)$ Group? $(\mathbb{Q}, \cdot)$

2 $\frac{1}{2}$

Def 1.2. The order 阶 of G is the number of elements of G. $|G|$.

$\mathbb{Z}_2 = \{[0], [1]\}$. $|\mathbb{Z}_2| = 2$.

$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$.

$|\mathbb{Z}| = +\infty$. finite group

Def 1.3. If $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$, then G is a commutative or abelian group.

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$.

<u>Def 1.4</u>. A subset $H \subset G$ is a subgroup of G under the law of composition of G. H is subgroup if

(1) $\forall h_1, h_2 \in H$, $h_1 h_2 \in H$.

(2) $\forall h \in H$, $h^{-1} \in H$. $\Downarrow$ $\Uparrow$

- $h_1 h_2^{-1} \in H$, $\forall h_1, h_2 \in H$

$\Rightarrow$ (2) $\forall h \in H$, $h^{-1} = e h^{-1} \in H$

(1) $h_1, h_2 \in H$, $h_1 h_2 \in H$?

$\Rightarrow h_2^{-1} \in H$ $\qquad h_1 (h_2^{-1})^{-1} \in H$.

$= h_1 h_2$

$(\mathbb{Z}, +) \leq (\mathbb{R}, +)$

§2. The Cyclic Group.

§2.1. Cyclic group.

G. $\quad g \cdot g \cdot g \cdots g =: g^n$, $\quad n > 0$

$g^{-1} \cdots g^{-1} = g^n$, $\quad n < 0$.

$e =: g^0$ $\quad n=0$

- $\boxed{g^{m+n} = g^m \cdot g^n, \quad (g^m)^n = g^{mn}, \quad \forall m,n \in \mathbb{Z}.}$

$\forall g \in G$,

$$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \}.$$

is called the group generated by g.

Def 2.1. A group G is called cyclic group if there exists a $g \in G$ s.t. $G = \langle g \rangle$.

- generating element usually not unique.
- Cyclic group is abelian.

  $g^m \cdot g^n = g^n \cdot g^m$ ✓

Exam 2.1.

- $\{e\}$.
- $(\mathbb{Z}, +)$ $\quad 1.$ $\quad \forall n \in \mathbb{Z}, \quad n = n \cdot 1$

  $$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

  $-1 \quad \forall n \in \mathbb{Z}, \quad n = (-n) \cdot (-1).$

$\bullet\ (\{2^n,\ n\in\mathbb{Z}\},\ \cdot) = \langle 2\rangle = \langle \tfrac{1}{2}\rangle$

$\bullet\ \mathbb{Z}_p = \{0, 1, \dots, p-1\}. = \langle 1\rangle.$

p is prime, $\boxed{\mathbb{Z}_p = \langle n\rangle}$, $n\in\{0,1,2,\dots,p-1\}.$

$$\boxed{(p,q)=1. \Rightarrow \exists\ k,l\in\mathbb{Z},\ s.t.\ kp+lq=1}$$

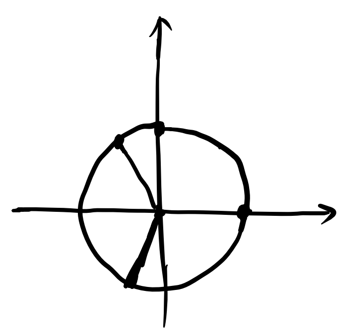
$\langle n\rangle \le \mathbb{Z}_p$

$\forall\ a\in\mathbb{Z}_p \Rightarrow a\in\langle n\rangle$ ($kn = lp + a.$

$(n,p)=1 \Rightarrow kn+lp=1.$

$\Rightarrow akn = -alp + a.$

$\bullet\ (\{e^{\frac{2\pi k i}{n}},\ k=0,1,\dots,n-1\},\ \cdot)$



order of g_0

$|G| < \infty.$ $\quad \sigma(g_0) = |G|$

Thm 2.1. Let G be a group generated by g_0. $|G|<\infty$. Then

(1) g_0^n, $n=0,1,\dots,|G|-1$ are all distinct elements.

(2) $\boxed{g^{|G|} = e, \ \forall g \in G.}$

Pf. (1) Prove by contradiction.

$\exists \ n_1, n_2 : \quad 0 \le n_2 < n_1 \le |G| - 1$

$g_0^{n_1} = g_0^{n_2}$

$\Rightarrow \quad g_0^{n_1 - n_2} = e. \qquad$ Let $|G| > q = n_1 - n_2 > 0$

$\forall n \in \mathbb{Z}, \quad n = kq + r, \ \exists k \in \mathbb{Z}, \ 0 \le r < q.$

$g_0^n = g_0^{kq+r} = (g_0^q)^k \cdot g_0^r = g_0^r, \qquad r = 0, 1, 2, \cdots, q-1$

$\Rightarrow \quad |G| \le q < |G|, \quad$ contradiction $\boxed{V}$

(2) $\boxed{g_0^{|G|} = e}, \quad g_0^{|G|} = g_0^m \Rightarrow g_0^{|G| - m} = e = g_0^0.$

$\Uparrow$

$\Rightarrow \quad m = 0.$

$\forall g \in G, \quad \exists \ n, \quad g = g_0^n$

$\Rightarrow \quad g^{|G|} = (g_0^n)^{|G|} = g_0^{n|G|} = (g_0^{|G|})^n = e.$

Thm 2.2. Every subgroup of a cyclic group is cyclic.

$(\mathbb{Z}, +) = \{ \dots -2, -1, 0, 1, 2, \dots \}$.

$\{ \dots, -4, -2, 0, 2, 4, \dots \} = \langle 2 \rangle$.

Pf. $H \subset G = \{e, a, \dots, a^{|G|-1}\}$.

Let q be the smallest non-zero positive integer s.t.

$$a^q \in H.$$

For any $c \in H$, $\exists\, n \in \{0, 1, \dots, |G|-1\}$, s.t. $c = a^n$.

$n = kq + r$, $\exists\, k \in \mathbb{Z}$, $0 \le r < q$.

$\Rightarrow \quad c = a^n = a^{kq+r} = (a^q)^k \cdot a^r$.

$\Rightarrow \quad a^r \in H$

$\Rightarrow \quad r = 0$.

$\Rightarrow \quad c = a^n = a^{kq} = (a^q)^k$

$\Rightarrow \quad H = \langle a^q \rangle$.

order

$|G|$

$o(g) = n$

$g^0, g^1, \dots, g^{n-1}, g^n = e$

$\Rightarrow \quad g^n = e$ smallest n

§2.2 Symbols and Relations.

$\{e, a\}$ $\quad e \quad ea \quad eaa \quad aea \quad aaae = a^3e.$

$ea = ae = a \Rightarrow e$ identity.

$a^n = e \quad \{e, a, a^2, a^3, \ldots a^n\}.$

$\{e, h\} = \{e, a\}$

$eh = he = h \quad , e$

$h^n = e$